Divided rights in authorized domain

The invention relates to a method of controlling access to a content item in a system comprising a set of devices, the method comprising a step of associating at least one usage right with the content item.

The invention further relates to a client system comprising a set of devices, the client system being arranged to perform access control to a content item, with handling means for a usage right associated with the content item.

The invention further relates to a server system being arranged to perform access control to a content item, the server system further associating at least one usage right with the content item.

The invention also relates to a signal for carrying usage rights.

The invention also relates to a device arranged to perform access control to a content item, being able to handle a usage right associated with the content item.

Television and other content is increasingly becoming digital. Also, digital content can easily be transferred between devices which often are able to communicate with each other. This does present the end-user with a user-friendly system, where access to content is no longer limited to a single device, but content can be accessed from any device connected to some kind of (in-home) network.

It also poses a threat to the content owner that its content is copied or transferred unlimitedly. A digital rights management (DRM) system is designed to protect and regulate access to content. For the content owner, who often wants to impose strict rules on digital transfer of content to prevent unlimited digital copying, content protection by a DRM system is an important condition for the acceptance of digital content distribution to consumer households.

In several fora, like CPTWG (Copy Protection Technical Working Group, http://www.cptwg.org), DVB (Digital Video Broadcasting, http://www.dvb.org), and TV-Anytime (http://www.tv-anytime.org), discussions are going on how to make sure that high-

valued digital content cannot be redistributed illegally when it is accessed by consumers on devices connected to their in-home network.

In recent discussions within DVB-CPT (Copy Protection Technical module) and TV-Anytime RMP (Rights Management and Protection), the above problems are addressed under the title Authorized Domain (AD). An AD both respects the content provider's and consumer's interest, in the sense that the consumer has freedom to access and distribute the content within the AD, while at the same time the rights of the content owners and service providers are covered by introducing strict import and export rules to prevent unlimited digital copying the content across domains.

The DVB-CPT group has defined an AD as a set of DVB-CPCM (Copy Protection and Copy Management) compliant functional units, that controls the flow of content and the content format. The AD represents an environment of trust for the authorized use of copyrighted content. The AD may consist of several, potentially disconnected, segments of a user's home network. This includes the temporary connection of mobile devices, and virtual "connection" of different network segments (possibly operational at non-overlapping times) by portable media.

An AD offers a consumer unrestricted and uncomplicated access to legally acquired content within the AD. Consumers will expect that they can add devices, rights, and content to the domain. Consumers will also expect that they can access their content anywhere, anytime, and on each of their devices. In addition this may also hold for mobile devices, or for terminals outside the house, such as a television in a hotel room. In addition, users can be added and removed from a domain, for example because they change between households. Other users also expect to have access to the content, for example because they are friends during a visit, or because of fair use provisions.

On the other hand, content providers require strong limitations on content exchange especially via Internet redistribution. Therefore, the rights to content should be clearly defined and protected. For example, in the domain of TV systems, a content right (also called ECM in pay-TV context) describes what is allowed with said content, and a usage right (also called EMM in pay-TV context) authorizes a person to use a certain content right, and can also describe what a user is allowed to do with said content.

Example usage rights are a right to play content, a right to make a one generation copy, etc.

Both content rights and usage rights may also contain cryptographic keys.

For a more extensive introduction to the use of DRM in home networks, see F.L.A.J. Kamperman, S.A.F.A. van den Heuvel, M.H. Verberkt, Digital Rights Management in Home Networks, Philips Research, The Netherlands, IBC 2001 conference publication vol. I, pages 70-77.

It is obvious that content rights and usage rights represent a certain amount of value, and should be protected from unwanted duplication or unauthorized creation. This could be done using secure and encrypted communications and secure storage of these rights, which are only to be handled by tamper resistant software and/or hardware.

Content rights are not personalized, and can hence be transferred together with the content or offered by different servers.

However, usage rights are personalized. Depending on the business model or protection scheme usage rights can be tied to a device, to a medium such as a CD, to an AD, or to a person. The requirement for tamper-resistant handling makes it difficult to freely use or transfer the usage right for example between devices or when traveling.

A better solution is to protect usage rights with a digital signature. The usage right is signed by the content provider or a different authorized source using well-known public key signature technology. In such a solution, the content provider has a private/public key pair. The private key is required in the process of adding a signature to the public right. The private key is kept completely secret by the content provider. The validity of the signature, which protects the integrity of the public right, can be checked using the corresponding public key. Because the usage right is protected by the digital signature, it can be allowed outside tamper resistant environment.

To prevent illegal access to content, the usage right certificate should only be accepted by a (compliant) device if it can be verified (using its public key) that it originates from an authorized source. In addition, other conditions can be checked before accepting a certificate, such as whether the certificate belongs to the AD the right is intended for, or in the case of a person based AD whether the associated person is present.

Some digital usage rights may be usable only a limited number of times, for example a right to play back a piece of content three times, or a right to transfer the content to a different domain two times. This requires that the usage right itself contains a counting or revocation mechanism of some kind that is triggered each time that the right is used. However, any change due to the implementation of the counting mechanism in the usage right invalidates the signature. The signature can only be computed by the trusted third party, which is clearly a disadvantage.

In addition, the usage right may also contain a right to transfer content a single time to a different domain or user. Such a transfer right needs to be revoked after it has been used. Revocation or deletion of such a transfer right also invalidates the signature of the remaining usage right.

It is an object of the current invention to provide a method which allows that the usage right can be handled without invalidating the digital signature.

This object is thereby realized by a method according to the preamble that the method further comprises decomposing the usage right into a set of partial rights, and subsequently separately signing each one of the set of partial rights, resulting in a corresponding signature.

This method has the advantage that a usage right is now signed in elementary pieces, rather than as a whole. For example, the right to transfer the content to a different domain and the right to play back the content once in a particular AD, are each individually signed. When a partial right is used or transferred, it is still digitally signed, and so are any remaining rights.

An embodiment of the method according to the invention is described in claim 2.

Devices in the system are able to access such a signed partial right, and verify its validity, without requiring access to the complete usage right. Subsequently, the right can be exercised after successful validation.

An embodiment of the method according to the invention is described in claim 4.

Some partial rights can only be exercised a limited number of times, allowing control over the number of times the content item may be accessed. If a right can only be exercised a single time, it has the advantage that it can be separately revoked, deleted, or immediately marked as having been used.

An embodiment of the method according to the invention is described in claim 5.

The device can check revocation of a right before exercising it, thereby increasing the robustness against the use of obsolete rights.

This check, in which a tamper resistant device within the domain can be consulted, allows reliable revocation of rights.

An embodiment of the method according to the invention is described in claim 6.

The system of devices may make up a domain, e.g. as described above, of, for example, devices belonging to members of a single household, or having some other relation between the devices or their owners. Persons can be allowed to enter and leave a domain. Users can be identified for example by a personal smart card.

An embodiment of the method according to the invention is described in claim 9.

At least one device in the domain is allowed to add its signature to the combination of one of the partial rights and information containing at least the identification of itself and/or a different device or domain, validity information (length, type), and subsequently to transfer this right to a different device, possibly being a part of or representing a different domain.

This has the advantage that it is possible to track the history, redistribution channel, and original issuer of a transferred right.

Similarly, a device could be allowed to limit itself to sign the partial right only, as described in claim 10.

An embodiment of the method according to the invention is described in claim 12.

The device that transfers the right can be required to verify the compliance of the device that receives the right. It may also check with a third party whether the receiving device has not been revoked. The receiving device may perform similar checks on the originating device.

An embodiment of the method according to the invention is described in claim 13.

The device that transfers the right to a different device can locally revoke or delete the partial right.

An embodiment of the method according to the invention is described in claim 14.

A type of usage right is introduced, called an offer right, which represents an offer from a content provider. The offer right may contain the promise to transfer upon request a signed usage right from the content provider directly to a third party to be specified at a later stage. This allows the owner of the offer right to "transfer" a usage right at a later stage, while it allows the content provider verification of the usage of the right. Additional

restrictions can be introduced, such as a minimum or maximum delay between the offer right and the time of transfer.

The third party can be a different domain, but it could also be one of the devices owned by the user which is not or not always part of the domain. The third party can also be a device owned by someone else, but in current use by the owner of the transfer, for example during a visit, while traveling, or in a hotel room.

It is a further object of the invention to provide a client system according to the preamble where the usage right is a set of individually signed partial rights, and the client system is being arranged to verify individually and handle individually the partial rights.

It is a further object of the invention to provide a server system according to the preamble having means to decompose the usage right into a set of partial rights, the server system further has a signing part being arranged to subsequently separately sign each one of the set of partial rights, and is arranged to bundle the individually signed partial rights into a set.

It is a further object of the invention to provide a signal according to the preamble where the usage rights are split into partial rights, which are individually signed.

It is a further object of the invention to provide a device according to the preamble where the device is further arranged to handle the usage right which has been split into partial rights, each of the partial rights having a digital signature.

These and other aspects of the invention will be further described by way of example and with reference to the drawing, in which:

Fig. 1 schematically shows a system comprising devices interconnected via a network,

Fig. 2 is a digitally signed right according to the prior art,

Fig. 3 is a set of partial rights that are individually signed according to the current invention,

Fig. 4 is a right that has been transferred and signed by the issuer according to the current invention,

Fig. 5 shows the transfer of said right between two domains,

Fig. 6 shows a field associated with each right to indicate the required protection level,

Fig. 7 shows the communication of an individually signed right to a location outside the in-home network, and

Fig. 8 shows an offer right being used to request the transfer of a usage right from a provider to a location outside the in-home network.

Throughout the figures, same reference numerals indicate similar or corresponding features. Some of the features indicated in the drawings are typically implemented in software, and as such represent software entities, such as software modules or objects.

Fig. 1 schematically shows an in-home network system 100. Such a system typically includes a number of devices, e.g. a radio receiver, a tuner/decoder, a CD player, a pair of speakers, a television, a VCR, a tape deck, a personal computer, and so on. These devices are usually interconnected to allow one device, e.g. the television, to control another, e.g. the VCR. One device, such as e.g. a tuner/decoder or a set top box (STB), is usually the central device, providing central control over the others.

Content 130, which typically comprises things like music, songs, movies, TV programs, pictures, programming guide information, and the like, is received for example through a PC 106 or a residential gateway or set top box 101. The source could be a connection to a broadband cable network, an Internet connection, a satellite downlink and so on. The set top box 101, or any other device in the system 100, may comprise a storage medium S1 such as a suitably large hard disk, allowing the recording and later playback of received content. The storage S1 could be a Personal Digital Recorder (PDR) of some kind, for example a DVD+RW recorder, to which the set top box 101 is connected. Content can also be provided to the system 100 stored on a carrier 120 such as a Compact Disk (CD) or Digital Versatile Disk (DVD). The content can then be transferred over the network 110 to a sink for rendering.

A sink can be, for instance, the television display 102, the portable display device 103, the mobile phone 104, and/or the audio playback device 105. The exact way in which a content item is rendered depends on the type of device and the type of content. For instance, in a radio receiver, rendering comprises generating audio signals and feeding them to loudspeakers. For a television receiver, rendering generally comprises generating audio and video signals and feeding those to a display screen and loudspeakers. For other types of content a similar appropriate action must be taken. Rendering may also include operations

such as decrypting or descrambling a received signal, synchronizing audio and video signals and so on.

Under certain conditions a personal computer 106 could also operate as source, storage medium, and/or sink.

The portable display device 103 and the mobile phone 104 are connected wirelessly to the network 110 using a base station 111, for example using Bluetooth or IEEE 802.11b. The other devices are connected using a conventional wired connection. To allow the devices 101-106 to interact, several interoperability standards are available, which allow different devices to exchange messages and information and to control each other. One well-known standard is the Home Audio/Video Interoperability (HAVi) standard, version 1.0 of which was published in January 2000, and which is available on the Internet at the address http://www.havi.org/. Other well-known standards are the domestic digital bus (D2B) standard, a communications protocol described in IEC 1030 and Universal Plug and Play (http://www.upnp.org).

It is often important to ensure that the devices 101-106 in the home network do not make unauthorized copies of the content. To do this, a security framework, typically referred to as a Digital Rights Management (DRM) system is necessary. Such a system typically uses rights. Different type of rights are content rights and usage rights.

A content right describes what is allowed with said content, and a usage right authorizes a person to use a certain content right, and can also describe what a user is allowed to do with said content.

Example usage rights are a right to play content, a right to make a one generation copy, etc.

Both content rights and usage rights may also contain cryptographic keys.

Secure processing and storage of rights can be done in a tamper resistant module 108 which can be located for example in the central controller 101.

Fig. 2 shows how a usage right can be signed according to the prior art. The usage right could for example comprise a render right, a transfer right, a derivative work right, or a utility right. Some rights could have limited validity in time, or in number of times. In this example, a usage right 201 might contain a render right 202 which specifies that a user has play rights to a certain piece of content, and a transfer right 203 which specifies that the user has a right to transfer a certain amount of content to a different domain exactly two times. The signing process makes use of well-known public key encryption is based on the existence of a pair of a private key and a public key. The private key is kept secret by the

party that signs and authenticates a message using this private key, and the corresponding public key can be distributed to and used by any third party in order to verify that the message has indeed been signed and not changed since it was signed by the originating party.

In this example, a private/public key pair generator 210 has generated a pair of a private key 211 and a public key 212 for the issuer of the usage rights, which can be the content provider itself whom we refer to as P. P uses its private key 211 during the signing process 213 of the usage right 201 and computes a signature 204. The combination of the usage right 201 and the signature 204 constitutes the signed usage right 205 which can be stored and transmitted without risk for undetected tampering. Any third party is able to perform a verification procedure 214 whether message 205 is authentic using the public key 212. The answer is available as output 215.

However, as only the issuer of the rights is able to sign such a usage right 201, a right from this set cannot be deleted or handled separately, as this would invalidate the signature 204. Partial rights that have been available outside the protection of secure environments can not reliably be revoked either, as there is no control over (illegal) copies of such a partial right.

The current invention makes it possible that the usage right can be handled without invalidating the digital signature.

In a first embodiment of the invention, the usage right 201 is decomposed into partial rights, which are subsequently signed individually.

Fig. 3 shows a set of individually signed partial rights 330 according to the current invention. It contains a number of example partial rights 301, 311, 321, and possibly more. In system 350 under control of P, partial rights are signed. Private key 351 of P is again used in process 353 to sign partial right 301 in order to compute signature 302. The same signing process 356 is used to compute P's signature 312 of partial right 311, and so on. These signed rights together with optionally other signed rights form a new set of individually signed partial rights 330. Each partial right can now be verified individually in the system 345 as in verification process 354, 357, and 360 to compute whether the signatures are valid (output 355, 358, and 361 respectively). This verification can be done by any device in the domain that has access to a partial right. Such a device may check whether the right has not been revoked by the issuer, or whether the issuer itself has not been revoked.

By treating the partial rights as a set, communication is minimized in size and number of transactions, and the conceptual relationship between the usage right and the content item is maintained.

Optionally, the complete set of individually signed partial rights 330 can be signed in process 373 as a whole to be able to verify completeness of the set of rights. Signing can be done again in a system 369 by the service provider but also, as shown in Fig. 3, by a different trusted third party T with its own private/public key pair 371/372 generated by key pair generator 370. Verification 374 yields the output answer 375 whether the signed set of rights 340 is complete.

An advantage of the first embodiment of the invention is that the partial rights are individually protected by a signature and can hence flow freely and independently within the domain. They can now individually be processed, e.g. revoked.

In a variation of the first embodiment, the complete set of individually signed partial rights can be signed in process 373 by the private/public key pair 371/372 of the receiver of the set of rights (e.g., the user) itself. The result can be sent back to, for example, the issuer of the set of rights. This can be part of a transaction, in order for the issuer to be able to prove that the complete set of rights has reached the intended receiver.

In a second embodiment of the invention, some or all of the signed partial rights are allowed to be transferred from a domain (the originating domain) to a different domain (the receiving domain).

Fig. 4 shows how a partial right, such as described in Fig. 3, is supplemented with additional information and signatures and subsequently signed to form a right to be transferred, further to be referred to as a transferable right. The transferable right is composed preferably from within the mentioned tamper resistant module, such as module 108 in Fig. 1. It contains the partial right 311, it further contains the original and still valid signature 312 created by the signing process 356 by P. In addition, metadata 411 is added containing information about but not limited to an identifier for the originating domain, an identifier for the receiving domain, the reason or purpose of transfer, time of transfer, and length of validity. For the identifier of the originating and receiving domain it is preferable to use their respective public keys. The partial right 311, the corresponding signature 312, and additional information 411 are composed together into information 430, and subsequently signed by the originating domain in process 463 with its own private key 461 to form signature 431. The transferable right 440 contains both information 430 and signature 431, and the validity and authenticity thereof can be verified in process 464 by any third party by using the public key 462 of the originating domain.

Fig. 5 shows two domains 500 and 550, both similar to system 100 in Fig. 1. It shows a transferable right 440 being transferred in process 540 outside domain 500, possibly

using secure communication, to a different domain 550, preferably after the communicating devices 101 and 501 in the respective domains have verified each other to be compliant and not revoked. The originating domain 500 can locally revoke or delete the transferred right.

This embodiment of the invention has the further advantage that both the originating domain and the target domain of a transferred right can be reliably retrieved from the metadata and signatures contained in the transferable right. This enables tracking of content.

In a third embodiment of the invention, a distinguishment is made between different protection levels for different types of rights and their handling.

Some of the partial rights can be freely used within a domain, even outside the protection of encrypted transmission or secure storage, such as a local right to play a certain piece of content. These rights will be called "safe rights". Safe rights can flow freely within the authorized domain (AD). Other rights, such as a right to transfer a piece of content exactly once, have to be revoked or deleted immediately after having been used. These rights will be called "weak rights". Weak rights need protection from unauthorized duplication and tampering, and to enforce for example that they can only be issued a limited number of times. This protection can for example be provided by not allowing weak rights outside the protection of a secure environment, for example in a tamper resistant module (possibly in a central controller) that also takes care of the transfer of rights to a different domain. It is of course also possible to define more than two protection levels.

A potential method to indicate the level of minimum protection required for a certain right, is to add a field with said information. Fig. 6 shows a modified set of rights 640, similar to the signed set of individually signed partial rights 340 in Fig. 3. In its simplest form, an additional single bit field 601/611 indicates whether the rights 301/311 have to be constricted in secure storage. For example, right 301 could be a play right which does not require secure storage (example content in bit field 601 is 0), while right 311 requires secure storage (example content in bit field 611 is 1). Alternative methods to indicate the required minimum protection level include but are not limited to: a device makes a decision on the protection level acquired based on the type of right, or a device has an (updateable) list which indicates for each right the required protection level.

The minimum required protection level can be used to determine how the partial right should be handled.

In a fourth embodiment of the invention, the transfer of a right outside the domain, in order to (perhaps temporarily) extend the in-home network with a device located

near the user/owner, is described. The extension can also be a device of a different owner who is entitled to access said content, as specified in the partial right or for other reasons (such as fair use).

In the European patent application having application number 02079390.7 (attorney docket NL021063) an extension of the AD framework is described which allows a person to view or use his personal content remotely outside the original definition of in-home network, for example when traveling. In said application, security is obtained by the encryption of content, by the secure storage of the corresponding decryption keys, and by personalized usage rights which are protected by a signature created by a trusted third party.

In such a situation it is advantageous to be able to communicate only parts of the usage right, which is possible using the individual signatures according to the current invention. Fig. 7 illustrates the transfer process 730 of a transferable right 731 from a system 100 (as shown in Fig. 1), to a remote hotel television system 770 via a gateway 751 to, for example, an audio set 753 or a television 752 located near the authorized user. These devices can be located in a hotel room, lounge, etc.

In a fifth embodiment of the invention, the transfer rights are kept at the service provider and the owner communicates to the service provider that the right should be transferred to another person or domain.

To indicate the existence of the transfer rights, the offer right has been introduced in the text of this application.

In this case secure storage is not required to prevent unauthorized duplication as the service provider may monitor that only an allowed number of copies can be made.

Fig. 8 shows the use of an offer right by an in-home network system 100. During a communication process 820 an offer right 821 is sent to a provider 810 in order to request the transfer 830 of a usage right 831 to a system 550 outside the in-home network. The service provider may either keep the transfer rights in storage 811 or generate them with a generator 812 when required.

Alternatives are possible. In the description above, "comprising" does not exclude other elements or steps, "a" or "an" does not exclude a plurality, and a single processor or other unit may also fulfill the functions of several means recited in the claims.